REMARKS

Pending Claims

Claims 1-17 and 19-20 are pending in this application. Claim 18 has been canceled without prejudice or disclaimer. Claims 17-18 have been amended. No new matter has been added.

Priority Document

Applicants respectfully request acknowledgment of the certified priority document JP 2002-002935, filed on March 1, 2002. Enclosed is a copy of the serial no. post card filed with the application and indicating that the Certified Priority Document was filed with the original application papers.

Claim Rejections under 35 U.S.C. §§ 102 and 103

Claims 1-8, 17 and 19-20 have been rejected under 35 U.S.C. §102(e) as being anticipated by Blumenau et al., U.S. Publication No. 2002/0007445 (Blumenau).

Claims 9-10 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Blumenau in view of Li et al., U.S. Patent Publication No. 2003/0093509 (Li); and claims 11-16 and 18 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Blumenau in view of Sanada, of record. Applicants request reconsideration of the rejections for the following reasons.

Each of the independent claims has been amended to set forth that the different types of I/O commands requested for the network transportation ports include READ and WRITE, and further the access control setting information includes READ only enable or READ and WRITE only enable information for each of the network transportation ports. Further, the independent claims now require that the READ only or READ and WRITE only information is changed (by the manger in claims 1 and 17) and the controller controls to allow or deny access sent via the network based on said READ only or READ and WRITE only information. Support for the added limitations to the independent claims can be found in claim 18 and in the specification at page 10, last line to page 11, line 11 of the specification, for example, and Fig. 2 of the drawings.

In the present invention, the security of data stored in a second storage system 101 (Fig. 1) connected to networks 107 and 108 is ensured, even when the second storage system is directly connected to a network and an unspecified number of host computers can gain access to the hard disk drives of the second storage system. Access is controlled in the present invention by determining which I/O commands are authorized between a plurality of network transportation ports of the second storage system and the hard disk drives thereof.

For example, the controller of the second storage system has an access controller having an access controlling table (123) for storing access control setting information, which includes READ only enable or READ and WRITE only enable information for each of the network transportation ports, as shown in Fig. 2. The I/O commands that are to be authorized between each of the plurality of transportation ports 113, 114 and each of the plurality of

nonvolatile data storing means (103, 104, etc.) is controlled in accordance with the access control setting information. In particular, the access controllers (access control units 115, 116) interpret and execute I/O requests transmitted by the host computers such that when an I/O process is transmitted, the access controllers refer to the access controlling table that stores access authorization setting information in order to determine whether the I/O commands should be authorized between each of the plurality of transportation ports (113, 114) and each of the plurality of nonvolatile data storing means (103, 104, etc.).

Referring to FIG. 2 of the present application, access control setting information is shown as having been set in the access controlling table 123. Set in the columns of the table is the access authorization setting for each logical disk (201, 202 ... 203) with respect to each network port (204, 205), i.e. the I/O commands for which access from the network ports is authorized for each logical disk. With reference to Fig. 3, when the second storage system 101 receives and executes I/O commands from the host computer that reach the network ports of the second storage device, they are transmitted to the corresponding access controllers 115 and 116. The access controllers 115 and 116 extract a target logical disk number included in the I/O commands and refer to the access controlling table 123 via the table controller 125. The access controller reads contents of a corresponding field of the access controlling table from the logical disk number and the identifier of the network port and judges whether or not such I/O command is authorized. If it is authorized, then the I/O command is execute and if not, the access controllers 115 and 116 notify the host computer of a failure of the I/O command.

From the management console 124, an operator can issue a change request to the access controlling table 123. See Fig. 4, step 402 and page 14, lines 6-8 of the specification. As a result, access can be dynamically controlled in each network transportation port by changing of the access control setting information. Blumenau does not disclose or suggest this aspect of the claimed combination.

As shown in Figs. 1 and 4 of Blumenau, storage controller 27 includes a plurality of port adapters 35, 36, and a plurality of storage adapters 37, 38. When a port adapter 35 or 36 receives a storage access request from one of the hosts 22-25, the port adapter forwards a storage access request to the storage adapters 37, 38. One of the storage adapters 37, 38 responds to the storage access request by performing a logical-to-physical translation to determine where the data to be accessed resides on the storage devices, and reads the data from the storage devices and writes the data to the cache memory, for access by the port adapter.

In order to restrict the set of volumes that can be seen by any one host in Blumenau, the memory 77 of the port adapter 35 stores information defining a correspondence between hosts in the data processing system and the set of volumes accessible to each host through the port adapter. For example, a volume access table 80 and volume lists 81 are stored in the memory 77. The volume access table specifies a correspondence between hosts and respective lists of volumes accessible to the hosts. See paragraph [0079] of Blumenau. The information in the volume access table 80 and the volume lists 81 can be accessed by a system administrator viewing a display 91 and operating a keyboard 92 of a service processor

93. However, the manager does not change access control setting information that includes READ only enable or READ and WRITE only enable information for the network ports, as in the present invention.

In Blumenau, with reference to Paragraphs [0094] - [0096] and Fig. 4 cited in the Office Action, access is controlled by storage volume partitioning by named groups, as shown in Fig. 5 of the reference. In the present invention, access is controlled by determining which I/O commands are authorized between a plurality of network transportation ports of the storage system and the hard disk drives thereof. In Fig. 25 of Blumenau, access is controlled by volume partitioning by virtual ports
in which virtual host IDs are used in place of the volume group name shown in Fig. 5. In the method of using virtual ports for volume partitioning, one or more virtual ports are assigned by the system administrator to each of the hosts having access to one or more of the virtual ports. Preferably logical storage volumes can be accessed through a single virtual port by no more than one assigned host. See paragraph [0117] of Blumenau. Accordingly, neither the storage volume partitioning by named groups nor the volume partitioning by virtual ports in Blumenau discloses or suggest the invention as claimed in claims 1-8, 17 and 19-20. Therefore the rejection under 35 U.S.C. § 102(e) should be withdrawn.

Sanada, applied in combination with Blumenau to reject claims 11-16 and 18 (the limitations of claim 18 have been substantially included in the independent claims by the present amendment), does not make up for the deficiency in disclosure in Blumenau with respect to the independent claims. Sanada discloses a controller having a plurality of network

transportation ports connected to different networks and an access controller for processing I/O commands requested for the transportation ports, including an access controlling table for storing access control setting information which defines the I/O commands that are to be authorized between each of the plurality of transportation ports and each of the plurality of nonvolatile data storing devices. However, the access control setting information in Sanada, which defines the I/O commands that are to be authorized, does not include READ only enable or READ and WRITE only enable information for each of the network transportation ports as claimed by Applicants in the amended independent claims.

This shortcoming in the disclosure of Sanada is recognized in the Office Action, however the conclusion is reached that it would be obvious to a person of ordinary skill in the art to modify the storage assignment method of Blumenau to include the different types of I/O commands including READ and WRITE and to include access control setting information of READ only enable or READ and WRITE only enable information based on the teachings of Sanada. However, Sanada does not disclose including READ only enable or READ and WRITE only enable information as the access control setting information for each of the network transportation ports. Therefore, the combination of Blumenau and Sanada cannot lead one having ordinary skill in the art to the claimed invention without impermissible hindsight reconstruction of the prior art from the teachings of the present invention. Accordingly, Applicants respectfully assert that the rejection under 35 U.S.C. § 103(a) based on Blumenau in view of Sanada be withdrawn.

Li is relied upon for disclosing the steps of claims 9 and 10, wherein when a

frequency of judgment that access non-authorization to specific data stored in the nonvolatile data storing means exceeds a predetermined threshold, access from the plurality of transportation ports to the data is not authorized. However, Li does not make up for the deficiencies in Blumenau with respect to the invention set forth in the independent claims, as aforementioned. Accordingly, the combination of Blumenau and Li does not render the invention set forth in claims 9 and 10 unpatentable under 35 USC §103(a).

CONCLUSION

In view of the foregoing, Applicants respectfully request reconsideration and reexamination such that a timely Notice of Allowance can be issued in this case.

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

By _____
John R. Mattingly
Reg. No. 30,293
(703) 684-1120

JRM/so
Date: August 17, 2006